Panel Discussion: Evolving DoD Security Requirements for Cloud

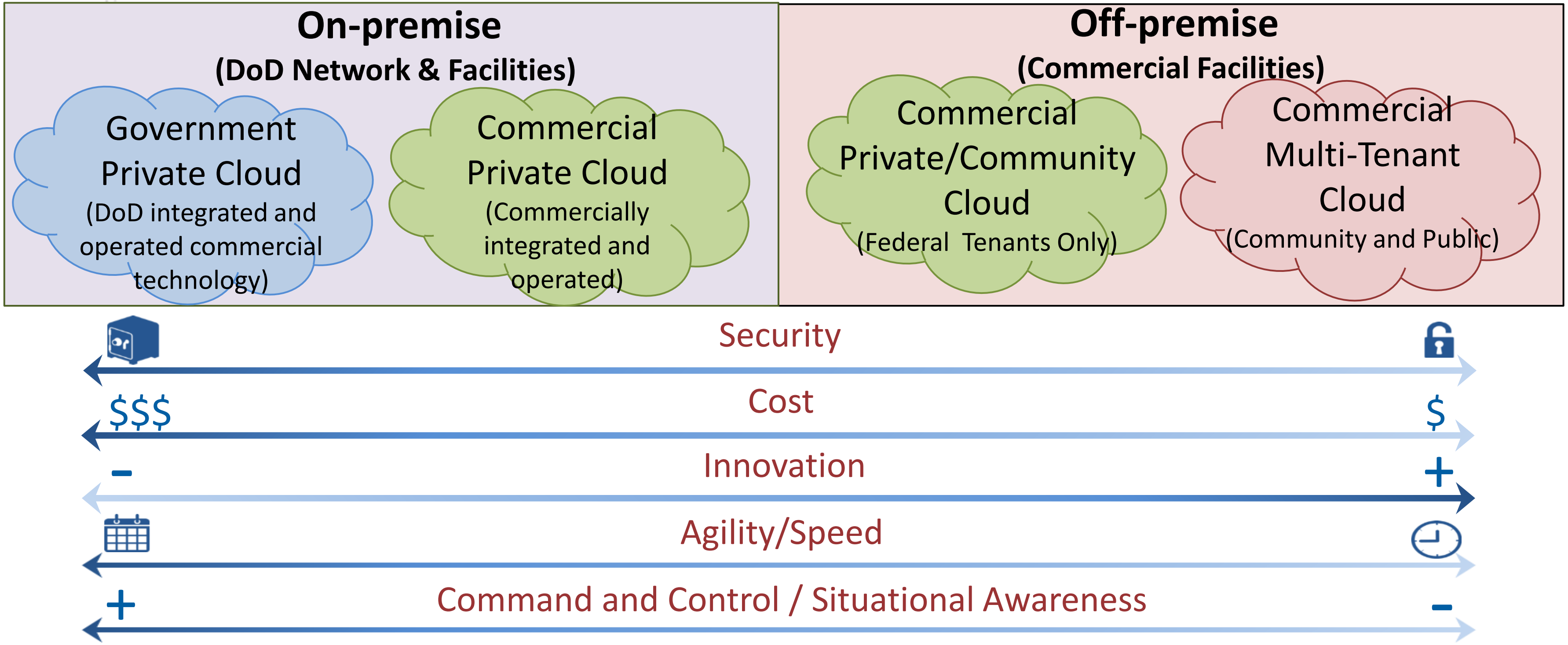
Roger S. Greenwell

Chief, Cybersecurity

29 January 2015

United in Service to Our Nation

Balancing Security and Risk



On-premise
(DoD Network & Facilities)

Government Private Cloud
(DoD integrated and operated commercial technology)

Commercial Private Cloud
(Commercially integrated and operated)

Off-premise
(Commercial Facilities)

Commercial Private/Community Cloud
(Federal Tenants Only)

Commercial Multi-Tenant Cloud
(Community and Public)

Goal: Improve leveraging of commercial capabilities and efficiencies while enabling effective risk management

DEFENSE INFORMATION SYSTEMS AGENCY

A Combat Support Agency

Cloud Security Controls

Ronald S. Rice

Cyber Standards Branch (RE71)

29 January 2015

United in Service to Our Nation

Information Impact Levels

- Information Impact Level - The combination of:
  1) The sensitivity of the information to be stored and/or processed in the cloud; and
  2) The potential impact of an event that results in the loss of confidentiality, integrity or availability of that information

- Cloud Computing SRG defines 4 Information Impact Levels
  - Cloud Security Model (CSM) defined 6 Information Impact Levels
  - Simplifies Impact Level selection and CSP capability matching
  - Levels 1 and 3 have been rolled up with the next higher level
  - Levels designated as Level 2, 4, 5, 6 for consistency with the old CSM

Security and Privacy Controls

- **FedRAMP v2 controls serve as minimum baseline for any authorization**
- **DoD FedRAMP+ controls based on a CNSSI 1253 categorization of M-M-x:**
  - **Moderate Confidentiality (M), Moderate Integrity (M), Availability (x)**
    - Availability addressed in the contract/SLA based on mission owner requirements
  - **CNSSI 1253 (2014) M-M-x Baseline**
    - NIST SP 800-53 rev4 Moderate Baseline PLUS CNSS tailored C/CEs
  - **FedRAMP v2, Moderate Baseline**
    - NIST SP 800-53 rev4 Moderate Baseline PLUS FedRAMP tailored C/CEs
  - **CNSSI 1253 & FedRAMP baselines compared to derive DoD's FedRAMP+ C/CEs**
- **Supplemental Control Requirements**
  - **CNSSI 1253 Privacy Overlay (when published) is invoked if PII/PHI is involved**
    - NIST SP 800-53 rev4 Privacy controls plus supplemental control guidance
  - **CNSSI 1253 Classified Overlay is invoked at Level 6**

Key Security Requirements

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises or AO authorized locations	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises or AO authorized locations	NIPRNet via CAP	Virtual / Logical PUBLIC COMMUNITY Strong Virtual Separation Between Tenant Systems & Information	ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Infrastructure	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Infrastructure	Favorably Adjudicated SSBI SECRET Clearance NDA

A Combat Support Agency

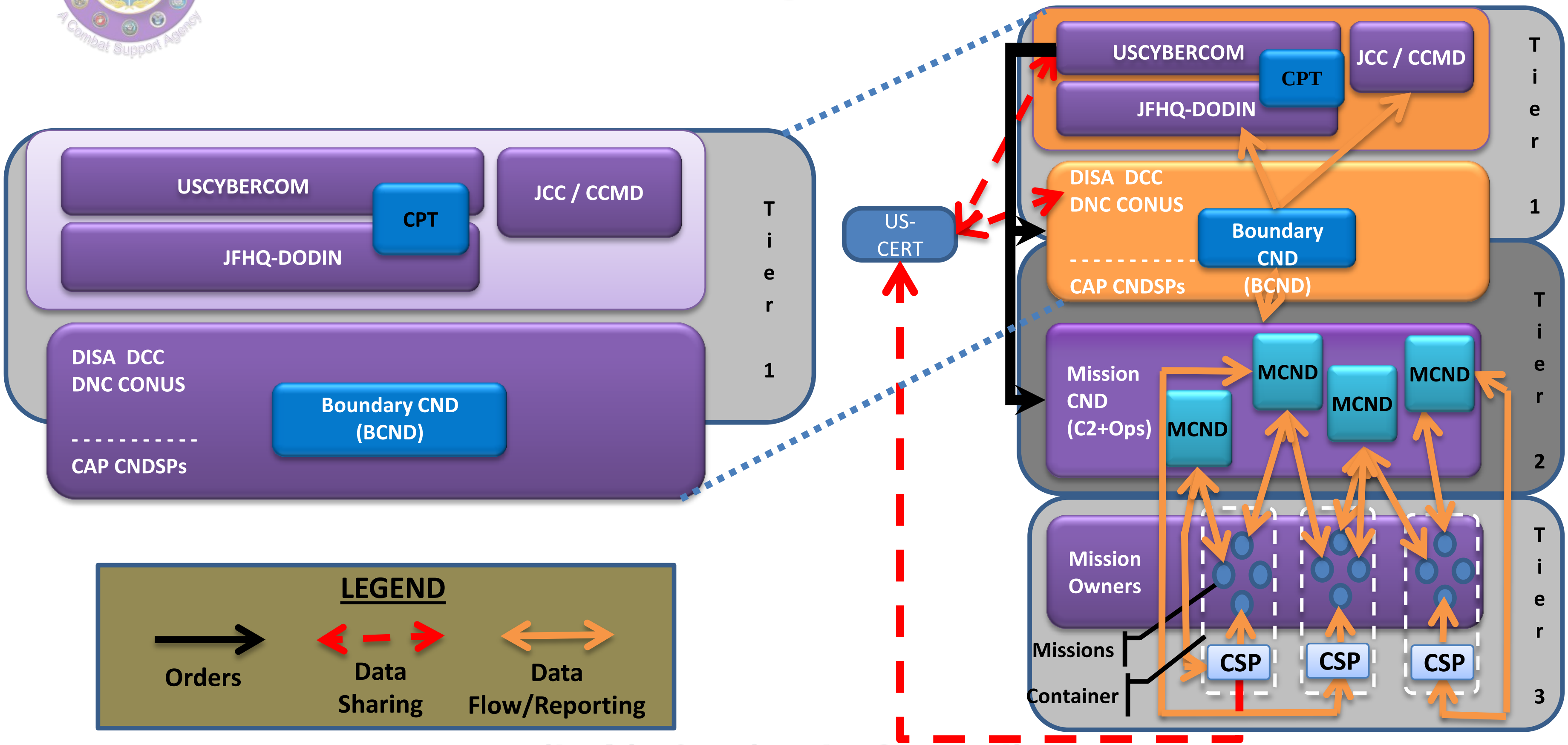
Cloud Computer Network Defense (CND)

Robert J. Mawhinney

Chief, CND Effectiveness Branch (RE61)

29 January 2015

Boundary CND Providers



USCYBERCOM

CPT

JFHQ-DODIN

JCC / CCMD

Tier 1

DISA DCC
DNC CONUS

Boundary CND (BCND)

CAP CNDSPs

US-CERT

USCYBERCOM

CPT

JFHQ-DODIN

JCC / CCMD

Tier 1

DISA DCC
DNC CONUS

Boundary CND (BCND)

CAP CNDSPs

Mission CND (C2+Ops)

MCND

MCND

MCND

MCND

Tier 2

Mission Owners

Missions

Container

CSP

CSP

CSP

Tier 3

LEGEND

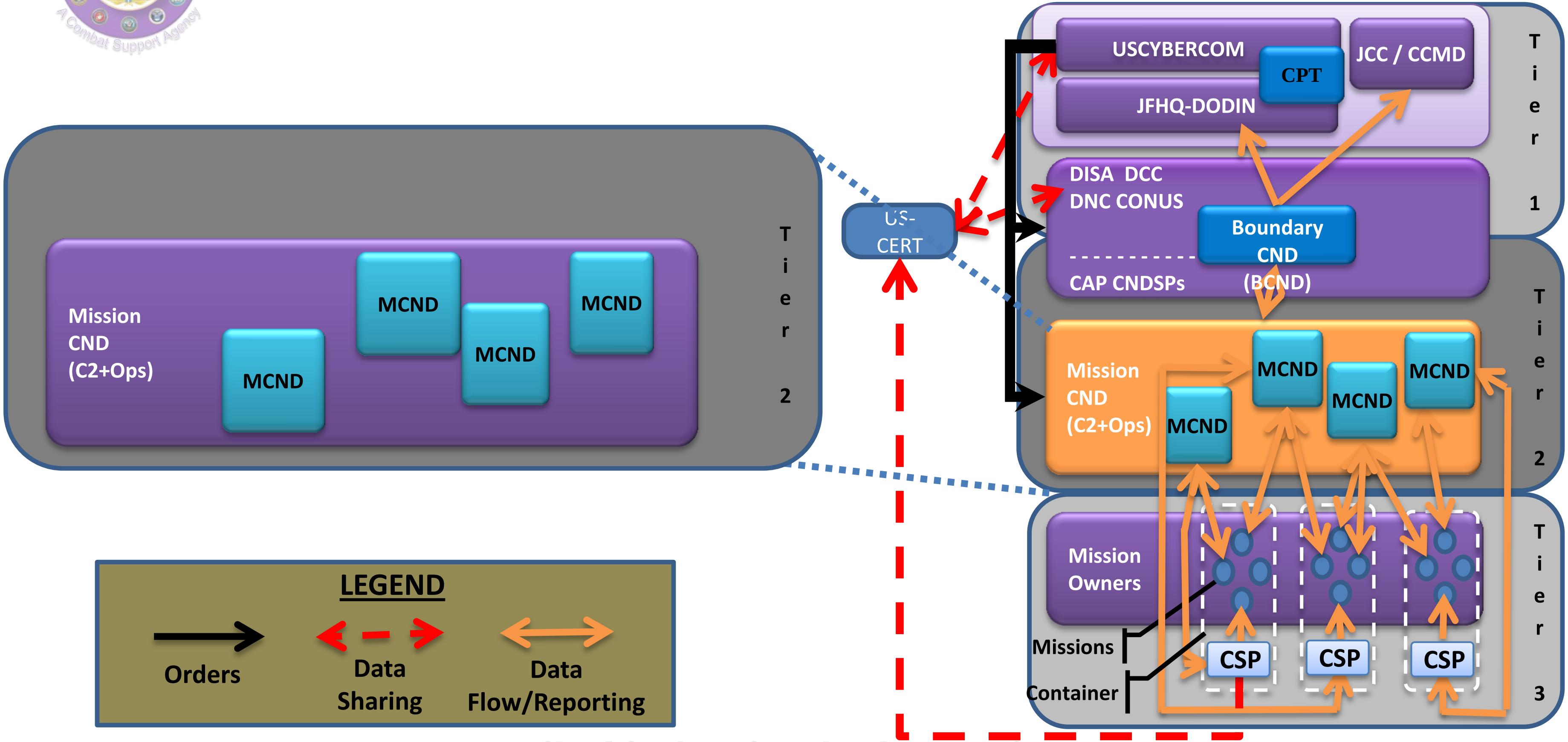
Orders

Data Sharing

Data Flow/Reporting

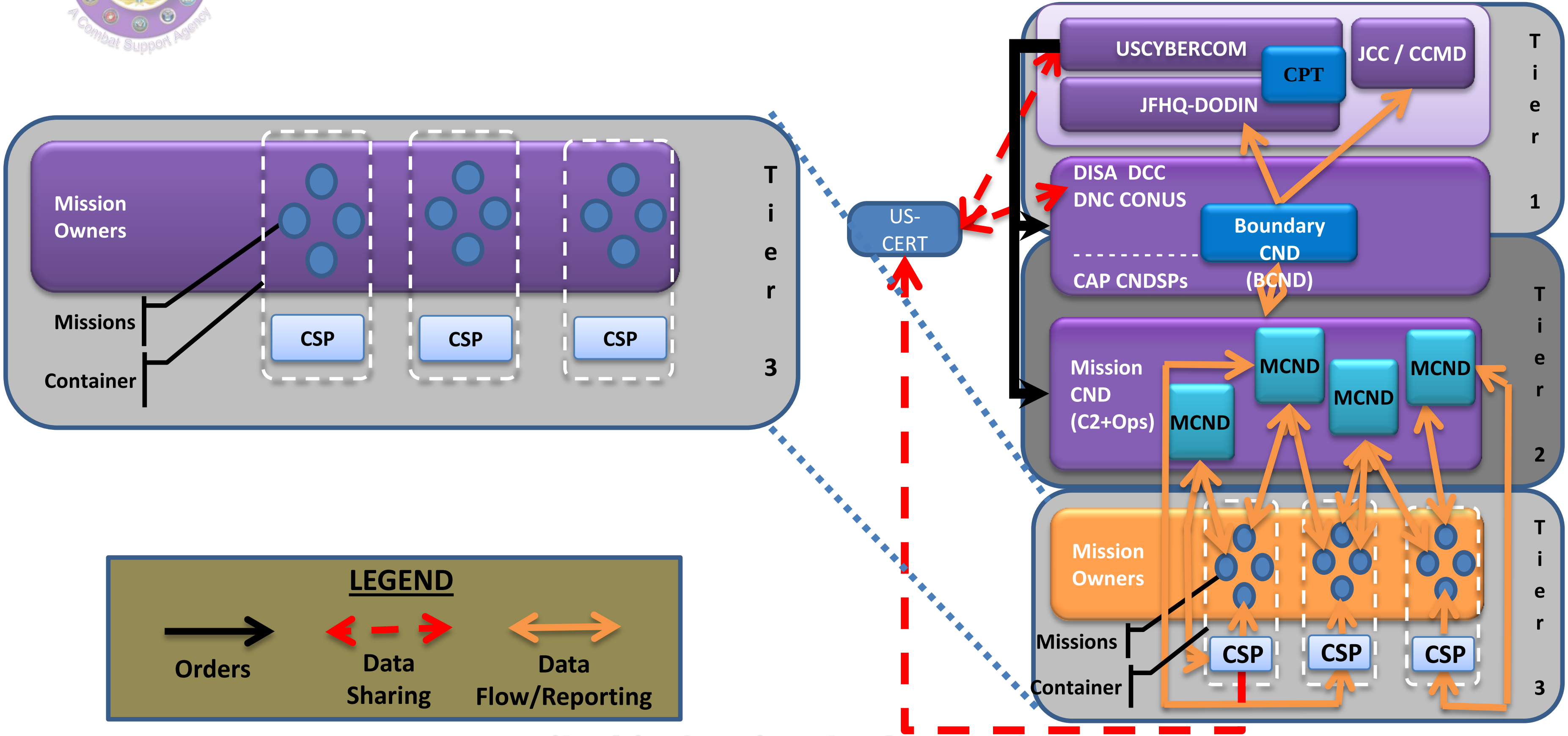
United in Service to Our Nation

Mission CND Providers



United in Service to Our Nation

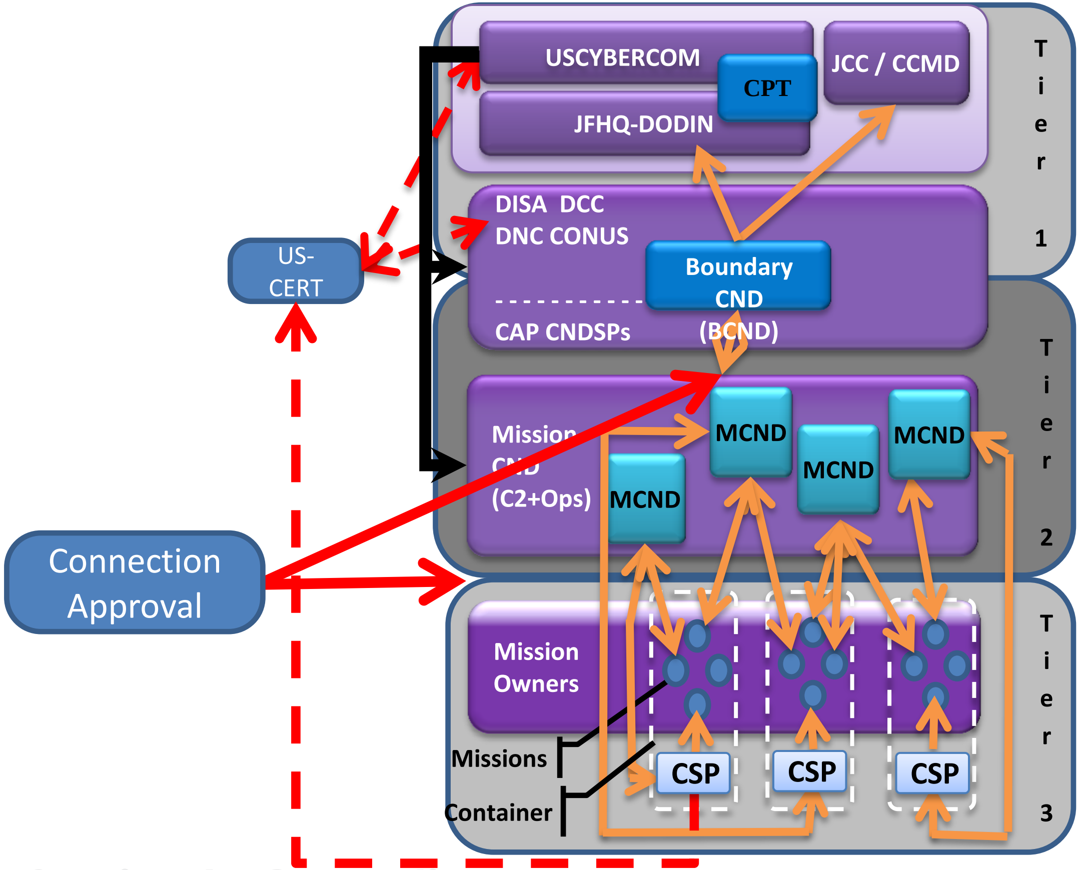
Mission Owners / CSPs



Connection Management

DISN Connection Approval Office

- Maintains the Connection Process Guide (CPG) to establish secure, dedicated connection to Cloud Service Offering
- Assures DoD Cloud Access Point (CAP) CND is established as part of issuing Authority to Connect
- Assures Impact Level considerations appropriate to the connection type
- Maintains a registry of all cloud operations for CND purposes



United in Service to Our Nation

A Combat Support Agency

Cloud Access Point (CAP)

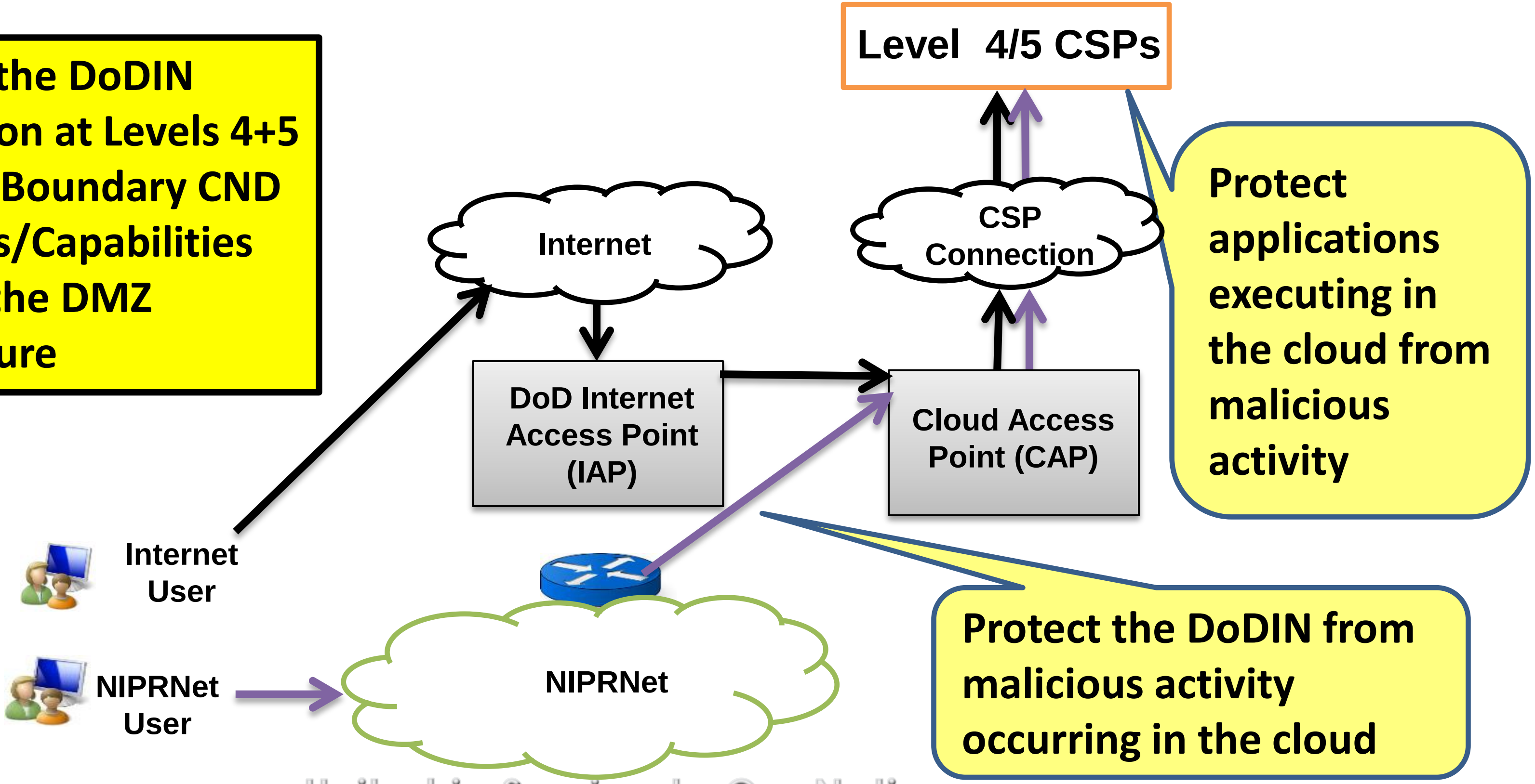
Peter T. Dinsmore

Risk Technology Executive (RE)

29 January 2015

Impact Level 4/5 Architecture

- Protects the DoDIN
- Connection at Levels 4+5
- Provides Boundary CND Functions/Capabilities
- Extends the DMZ architecture

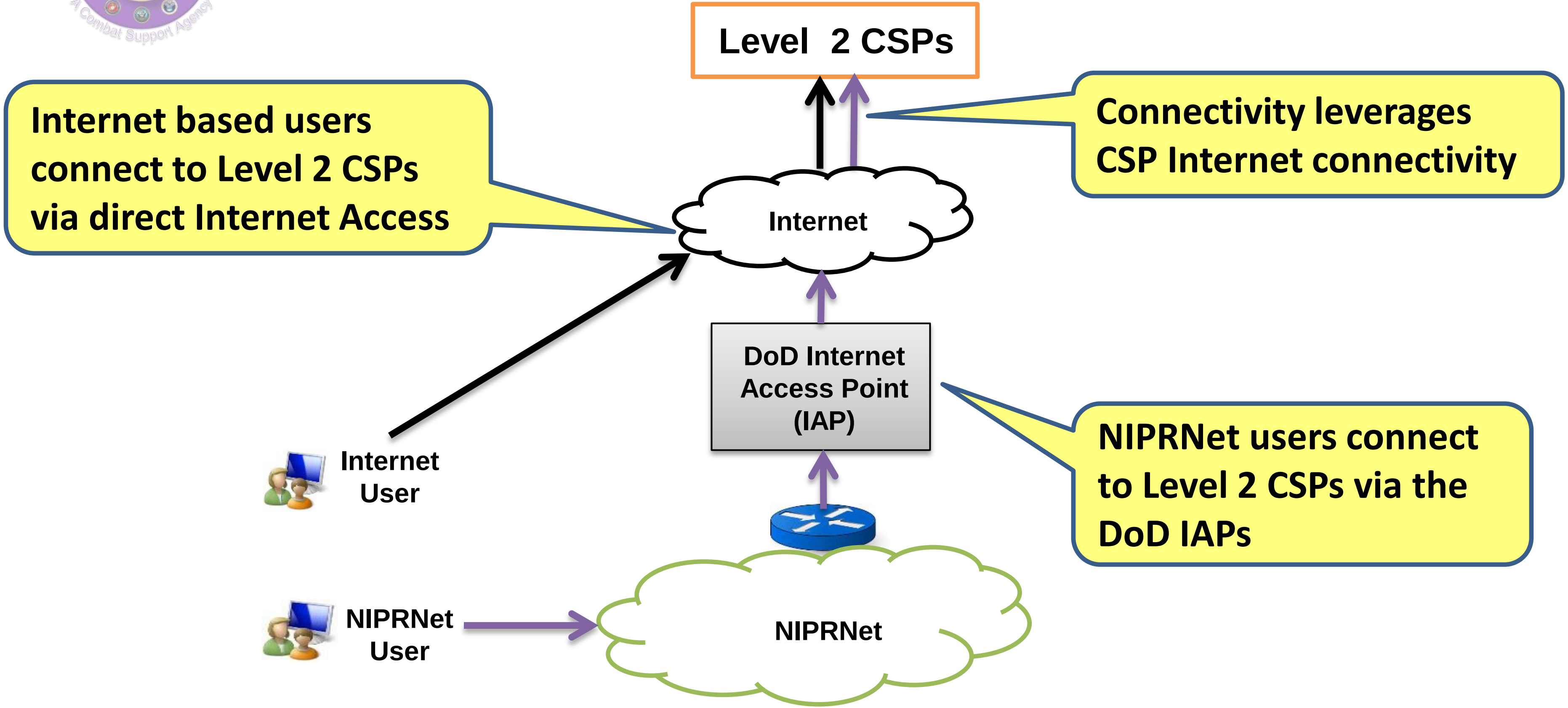


Protect applications executing in the cloud from malicious activity

Protect the DoDIN from malicious activity occurring in the cloud

United in Service to Our Nation

Impact Level 2 Architecture



Level 2 CSPs

Internet based users connect to Level 2 CSPs via direct Internet Access

Connectivity leverages CSP Internet connectivity

Internet

DoD Internet Access Point (IAP)

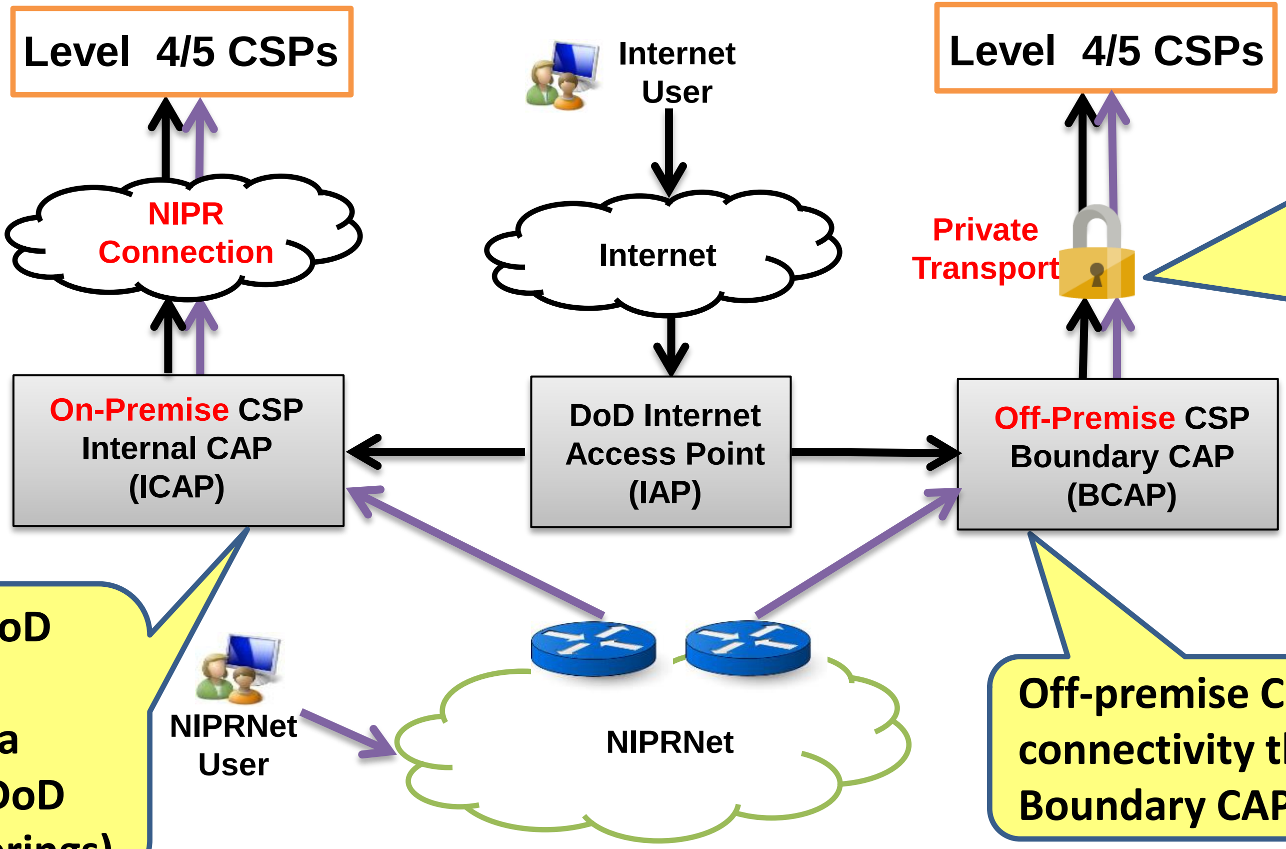
NIPRNet users connect to Level 2 CSPs via the DoD IAPs

Internet User

NIPRNet User

NIPRNet

On-premise vs. Off-premise


Level 4/5 CSPs
NIPR Connection
On-Premise CSP Internal CAP (ICAP)
Internet User
Internet
DoD Internet Access Point (IAP)
Level 4/5 CSPs
Private Transport
Off-Premise CSP Boundary CAP (BCAP)
NIPRNet User
NIPRNet

Meet Me' Points (MMP) will support multiple CSPs

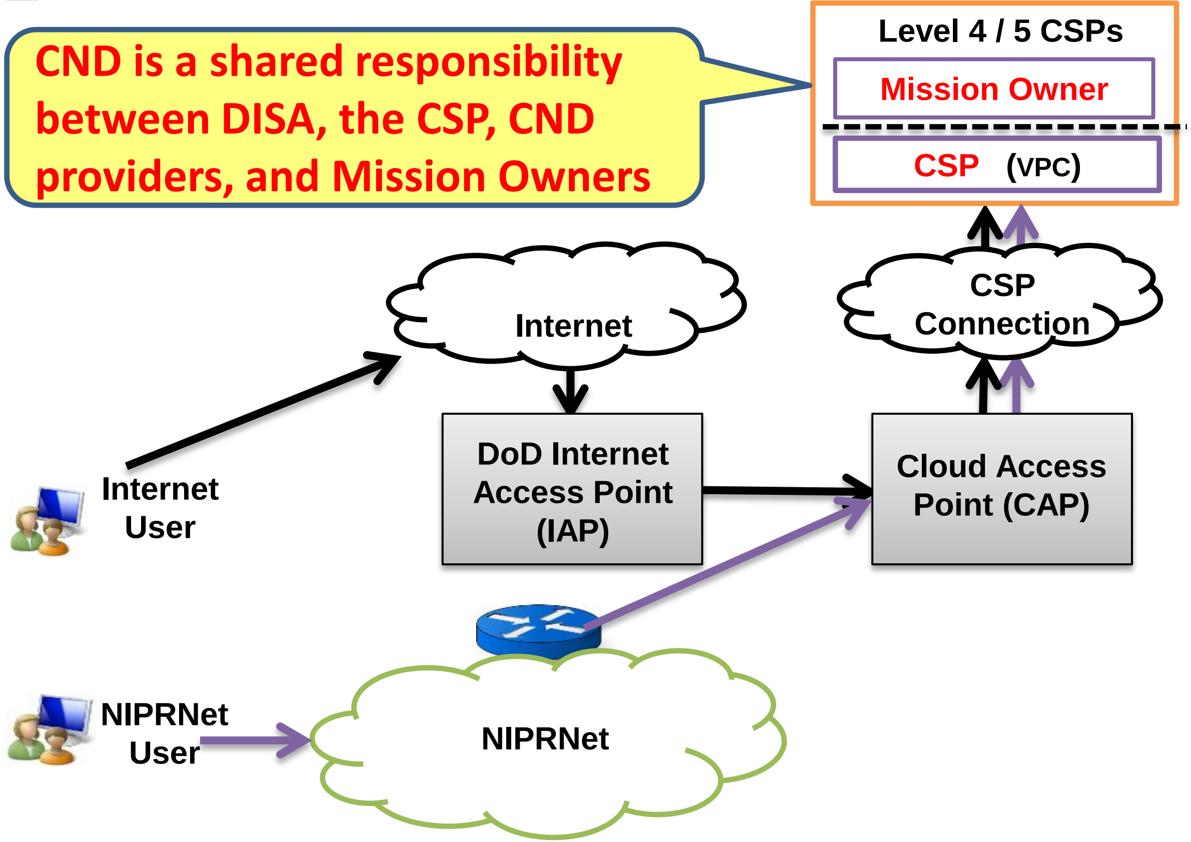
On-premise (DoD B/P/C/S) CSP connectivity via Internal CAP (DoD Dedicated Offerings)

Off-premise CSP connectivity through Boundary CAP

Infrastructure vs. Mission

ELEMENTS OF CND

- Intrusion Detection/Prevention System (IDPS)
- Firewall Capabilities
- Enterprise Information Assurance
- Enclave Security
- Application Protection
- Logging and Analysis



CND is a shared responsibility between DISA, the CSP, CND providers, and Mission Owners

Level 4 / 5 CSPs

Mission Owner

CSP (VPC)

CSP Connection

Internet

DoD Internet Access Point (IAP)

Cloud Access Point (CAP)

Internet User

NIPRNet User

NIPRNet

CAP Process and Procedures

- Connection of a mission system to the DoDIN via an ICAP or BCAP will be approved and recorded by the DISA Connection Approval Office in accordance with normal connection approval procedures
- Initial connections (physical or virtual) to a CSP's network will occur during onboarding of the CSP's first Mission Owner customer.
- Additional connections will be made or capacity will be scaled as more Mission Owners use the given CSP.

United in Service to Our Nation